Encryption with Delayed Dynamics

Toru Ohira
Sony Computer Science Laboratory
3-14-13 Higashi-gotanda, Shinagawa,
Tokyo 141, Japan
(Sony Computer Science Laboratory Technical Report: SCSL-TR-98-014)
(February 2, 2008)

We propose here a new model of encryption of binary data taking advantage of the complexity associated with delayed dynamics. In this scheme, the encryption process is a coupling dynamics with various time delays between different bits in the original data. It is shown that decoding of the encrypted data is extremely difficult without a complete knowledge of coupling manner with associated delays for all bits of the data.

Complex behaviors due to time delays are found in many natural and artificial systems. Some examples are delays in bio-physiological controls (*1*, *2*), and signal transmission delays in large–scale networked or distributed information systems (See e.g. (*3*, *4*)). Research on systems or models with delay has also been carried out in the fields of mathematics(*5*, *6*), artificial neural networks (*7*, *8*), and in physics (*9*, *10*, *11*). This series of research has revealed that time delay can introduce surprisingly complex behaviors to otherwise simple systems, because of which delay has been considered an obstacle from the point of view of information processing.

In this paper, however, we actually take advantage of this complexity with delayed dynamics and incorporate it into a new model of encryption. The encryption process is identified with a coupling dynamics with various time delays between different bits in the original data. We show that the model produces a complex behavior with the characteristics needed for an encryption scheme.

Let us now describe the encryption model in more detail. $\mathbf{S}(0)$ is the original data of N binary bits, whose ith element $s_i(0)$ takes values $+1$ or -1. The delayed dynamics for the encryption can be specified by a key which consists of the following three parts: (1) a permutation $\mathbf{P}$ generated from $(1, 2, 3, .., N)$, (2) a delay parameter vector $\vec{\tau}$ which consists of N positive integers, and (3) number of iterations of the dynamics T. Given the key $K = (\mathbf{P}, \vec{\tau}, T)$, the dynamics is defined as

$$s_i(t) = (-1) \times s_{p_i}(t - \tau_i), \tag{1}$$

where p_i and τ_i are ith element of $\mathbf{P}$ and $\vec{\tau}$, respectively. (If $t - \tau_i < 0$, we set $t - \tau_i = 0$.) In Figure 1, this dynamics is shown schematically. The state of the ith element of $\mathbf{S}(t)$ is given by flipping the state of the p_ith element of $\mathbf{S}(t - \tau_i)$. Thus this dynamics causes interaction between N bits of the data in both space and time. The encoded state $\mathbf{S}(T)$ is obtained by applying this operation of equation (1) iteratively T times starting from $\mathbf{S}(0)$.

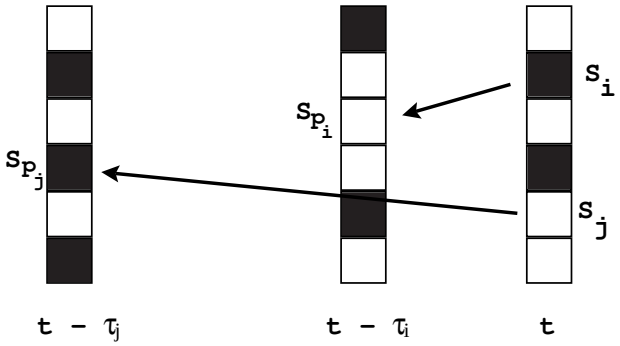
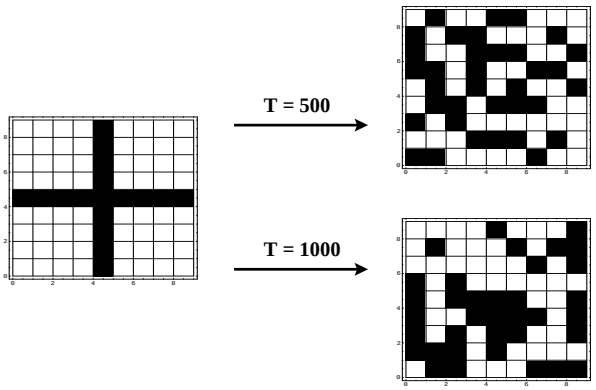


FIG. 1. Schematic view of the model dynamics. The state of the ith element of $\mathbf{S}(t)$ is given by flipping the state of the p_ith element of $\mathbf{S}(t - \tau_i)$.

We investigate numerically the nature of the delayed dynamics from the perspective of measuring the strength as an encryption scheme. First, we examine how the state $\mathbf{S}(t)$ evolves with time. In Figure 2 , we have shown an example of encoded states with different T using the same $\mathbf{P}$ and $\vec{\tau}$ for a case of $N = 81$. To be more quantitative, we compute the following quantity as a measure of difference between two encoded states at different times t and t_f:

$$Y(t) = \frac{1}{N} \sum_{i=0}^{N} S_i(t) S_i\,(t_f) \tag{2}$$

A typical example is shown in Figure 3. We note that the dynamics of our model has a property of occasionally very similar, but not exactly the same, states appearing indicated by sharp peaks in the figure. Except around these particular points, however, we generally obtain rather uncorrelated encoded states (i.e., $Y \approx 0$) with different iteration times. This is a desirable property of the model as an encryption scheme: the same state can be encoded into uncorrelated states by changing T.



$$\mathbf{P} = \begin{bmatrix} 4 & 33 & 62 & 49 & 47 & 26 & 20 & 7 & 21 \\ 65 & 72 & 57 & 73 & 67 & 75 & 25 & 34 & 40 \\ 60 & 12 & 70 & 10 & 14 & 43 & 38 & 17 & 29 \\ 51 & 46 & 77 & 81 & 52 & 45 & 31 & 54 & 39 \\ 76 & 71 & 30 & 44 & 28 & 16 & 13 & 8 & 56 \\ 1 & 78 & 22 & 19 & 24 & 18 & 61 & 74 & 59 \\ 55 & 66 & 64 & 53 & 27 & 80 & 63 & 68 & 5 \\ 3 & 23 & 11 & 9 & 79 & 58 & 35 & 42 & 15 \\ 50 & 41 & 48 & 37 & 36 & 6 & 2 & 32 & 69 \end{bmatrix} \qquad \tau = \begin{bmatrix} 2 & 10 & 4 & 2 & 6 & 10 & 3 & 7 & 4 \\ 3 & 2 & 8 & 6 & 6 & 7 & 5 & 10 & 2 \\ 3 & 1 & 5 & 1 & 1 & 1 & 3 & 1 & 8 \\ 10 & 8 & 2 & 6 & 4 & 4 & 9 & 5 & 7 \\ 9 & 4 & 8 & 2 & 10 & 2 & 6 & 2 & 5 \\ 2 & 5 & 1 & 3 & 2 & 7 & 1 & 5 & 10 \\ 2 & 8 & 2 & 1 & 8 & 2 & 4 & 8 & 10 \\ 10 & 5 & 6 & 5 & 9 & 10 & 4 & 1 & 9 \\ 8 & 3 & 5 & 9 & 3 & 3 & 4 & 1 & 1 \end{bmatrix}$$

FIG. 2. Examples of encoding with the model dynamics from an initial state to $T = 500$ and $T = 1000$ with $\mathbf{P}$ and $\vec{\tau}$

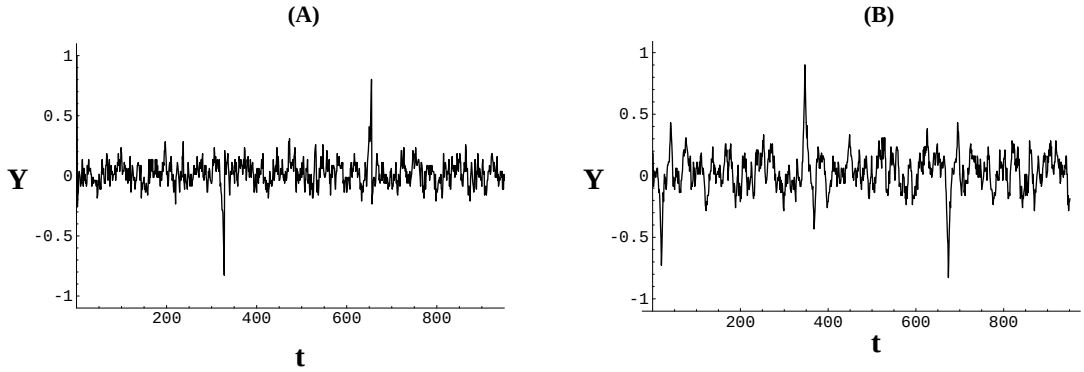


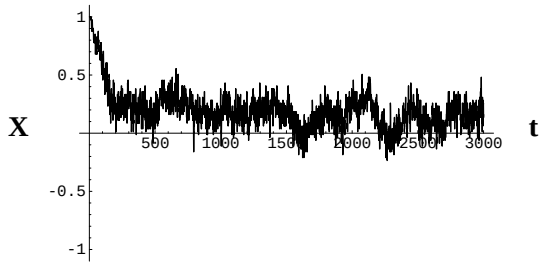
FIG. 3. Examples of the correlation Y between encoded states at different time steps evaluated by equation (2). Cases with (A) $t_f = 0$ and (B) $t_f = 1000$ are plotted with the initial state and $\mathbf{P}$ and $\vec{\tau}$ the same as in Figure 2.

Next, we investigated the effect of a minor change of $\mathbf{P}$ and $\vec{\tau}$ on the model dynamics. Starting with the same initial condition, we evaluate how two states $\mathbf{S}(t)$ and $\mathbf{S}'(t)$ are encoded with slightly different $\mathbf{P}$ and $\mathbf{P}'$, respectively, by computing

$$X(t) = \frac{1}{N} \sum_{i=0}^{N} S_i'(t) S_i(t) \tag{3}$$

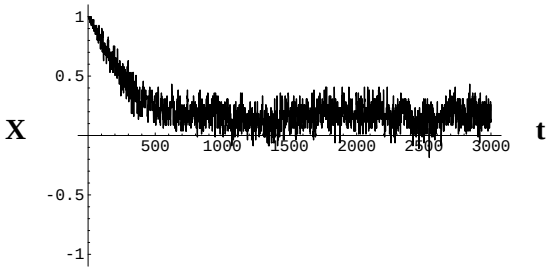
A representative result is shown in Figure 4. The same evaluation with $\vec{\tau}$ and $\vec{\tau'}$ is shown in Figure 5. These graphs indicate that if we take sufficiently large T, the same state can evolve into rather uncorrelated states with only a slight change of $\mathbf{P}$ and $\vec{\tau}$. This again is a favorable property in the light of encryption. It makes iterative and gradual

guessing of $\mathbf{P}$ and $\vec{\tau}$ in terms of their parts and elements very difficult: a nearly correct guess of the values of $\mathbf{P}$ and $\vec{\tau}$ does not help in decoding.



$$\mathbf{P'} = \begin{bmatrix} 4 & 33 & 62 & 49 & 47 & 26 & 20 & 7 & 21 \\ 65 & 72 & 57 & 73 & 67 & 75 & 25 & 34 & 40 \\ 60 & 12 & 70 & 10 & 14 & 43 & 38 & 17 & 29 \\ 51 & 46 & 77 & 81 & 52 & 45 & 31 & 54 & 39 \\ 76 & 71 & 30 & 44 & 28 & 16 & 13 & 8 & 56 \\ 1 & 78 & 22 & 19 & 24 & 18 & 61 & 74 & 59 \\ \boxed{3} & 66 & 64 & 53 & 27 & 80 & 63 & 68 & 5 \\ \boxed{55} & 23 & 11 & 9 & 79 & 58 & 35 & 42 & 15 \\ 50 & 41 & 48 & 37 & 36 & 6 & 2 & 32 & 69 \end{bmatrix}$$

FIG. 4. Example of the correlation X evaluated by equation (3) between two states encoded by slightly different $\mathbf{P}$ and $\mathbf{P}'$. The difference of $\mathbf{P}'$ from $\mathbf{P}$ is indicated by a box. The initial state and $\mathbf{P}$ and $\vec{\tau}$ are the same as in Figure 2.



$$\tau' = \begin{bmatrix} 2 & 10 & 4 & 2 & 6 & 10 & 3 & 7 & 4 \\ 3 & 2 & 8 & 6 & 6 & 7 & 5 & 10 & 2 \\ 3 & 1 & 5 & 1 & 1 & 1 & 3 & 1 & 8 \\ 10 & 8 & 2 & 6 & 4 & 4 & 9 & \boxed{10} & 7 \\ 9 & 4 & 8 & 2 & 10 & 2 & 6 & 2 & 5 \\ 2 & 5 & 1 & 3 & 2 & 7 & 1 & 5 & 10 \\ 2 & 8 & 2 & 1 & 8 & 2 & 4 & 8 & 10 \\ 10 & 5 & 6 & 5 & 9 & 10 & 4 & 1 & 9 \\ 8 & 3 & 5 & 9 & 3 & 3 & 4 & 1 & 1 \end{bmatrix}$$

FIG. 5. Example of the correlation X evaluated by equation (3) between two states encoded by slightly different $\vec{\tau}$ and $\vec{\tau'}$. The difference of $\vec{\tau'}$ from $\vec{\tau}$ is indicated by a box. The initial state and $\mathbf{P}$ and $\vec{\tau}$ are the same as in Figure 2.

With these properties of the model, an exhaustive search appears to be the only method for guessing the key. Even if one knows N and τ_{max}, the largest element in $\vec{\tau}$, one is still required to search for the correct key from among $(N!)(\tau_{max})^N$ combinations and to guess T. The commonly used DES (Data Encryption Standard) employs 2^{56} bit keys (*12*) . We can obtain a similar order of difficulty with rather small values of N and τ_{max}; for instance, $N \approx 11$ and $\tau_{max} \approx 10$ (*13*).

There are different methods possible for using this model for a secure communication between two persons who share the key. One example is that the sender sends a series of encoded data in sequence for the interval between T and $T + \tau_{max}$ (or longer). The receiver can recover the original data from this set of encoded data by applying a reverse dynamics with the key. In a situation where the data sent is a choice out of multiple data sets known to the receiver, the receiver can run the encryption dynamics to the entire sets with the key for case matching.

As in many dynamical systems in the presence of delay, the behavior of the model presented here is not analytically tractable as it stands. The model can be viewed as an extension of iterative function on a vector, or as an extension of cellular automata, with different delays for each element. Analytical and numerical investigation of the model from these perspectives as well as implementation of the model into a software tool is currently underway. It is hoped that the model presented here can serve to call attention to the issue of encryption from the standpoint of delayed dynamics studies taking place in various scientific disciplines.

REFERENCES AND NOTES

1. M. C. Mackey and L. Glass, *Science* **197**, 287 (1977);
2. A. Longtin and J. Milton, *Biol. Cybern.* **61**, 51 (1989);
3. P. Jalote, *Fault Tolerance in Distributed Systems.* (Prentice Hall, NJ, 1994).
4. N. K. Jha and S. J. Wang, *Testing and Reliable Design of CMOS Circuits.* (Kluwer, Nowell, MA, 1991).
5. K.L. Cooke and Z.Grossman, *J. Math. Analysis and Applications* **86**, 592 (1982);
6. U. Küchler and B. Mensch, *Stochastics and Stochastics Reports* **40**, 23 (1992).
7. C. M. Marcus and R. M. Westervelt, *Phys. Rev. A* **39**, 347 (1989);
8. J. A. Hertz, A. Krogh, and R. G. Palmer, *Introduction to the Theory of Neural Computation* (Addison–Wesley, Redwood City, CA, 1991).
9. M. W. Derstine, H. M. Gibbs, F. A. Hopf and D. L. Kaplan. Phys. Rev. A **26**, 3720 (1982);
10. K. Pyragas. Phys. Lett. A **170**, 421 (1992);
11. T. Ohira, Phys. Rev. E **55**, R1255 (1997).
12. For description of DES, see e.g., A. J. Menezes, P. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, 1996). A 2^{56} bit key scheme was recently revealed in an open challenge using many computers over the Internet. (http://www.rsa.com/pressbox/html/980226.html).
13. The search space increases rapidly in particular with the increase of N due to factorials.